Remarks:

Status of the Claims

The office action summary mailed with the office action of September 12, 2008 rejects claims 1-7, however, in the claim rejections under 35 USC 103(a) claim 8 is rejected. Applicants assume the office action summary listing claims 1-7 as rejected contained a typographical error and that claims 1-8 are rejected in the office action.

Claims 1-8 were rejected in the Office Action mailed September 12, 2008. Claims 1-8 are objected to. Claims 1, 2, 4 through 6 and 8 are amended herein. Claim 9 is added herein. Claim 3 and 7 are cancelled herein. Claims 1-2 and 4-6, 8 and 9 are now pending in the application.

The Claims

Claim Objections

Claims 1-8 were objected to because of the following informalities: The claims recite a method "characterised" and should be corrected to read "characterized". Appropriate correction is required.

Applicants have amended the claims to replace characterised with characterized.

Claims 5 and 7 are objected to under 37 C.F.R. 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim.

The claim dependencies have been amended to overcome improper multiple dependencies.

Applicants posit that all objections to claims are now moot and respectfully request withdrawal of the objections.

35 USC 101

Claims 6-7 stands rejected under 35 USC 101 as being directed to non-statutory subject matter as they do not fall under any of the statutory classes of inventions. The language in the claim raise an issue because the claims are directed merely to an abstract idea that is not tied to an article of manufacture which would result in a practical application producing a concrete, useful and tangible result to form the basis of statutory subject matter under 35 USC 101.

The claims could reasonably be drawn to function descriptive material, per se, i.e. "program" may be taken to mean software alone, and as such the claims would be directed to non-statutory subject matter.

Claims 6 has been amended herein. Applicants posit that Claim 6 as amended clearly point to statutory subject matter and respectfully request the withdrawal of the rejection under 35 USC 101. A claim may be considered statutory subject matter if the claim recites a process that (1) it is tied to a particular machine or apparatus, or (2) it transforms a particular article into a different state or thing." *In re Bilski,* Slip op. at 10 and 11 (Fed. Cir. 2008). Claim 6 is drawn to "A method to secure an electronic assembly implementing a calculation process." Thus, it transforms a particular article (the electronic assembly) from one state (insecure) to a different state (secure). The electronic assembly is transformed by performing the recited process steps. Therefore, Claim 6 satisfies the requirements for statutory subject matter recently set forth by the Court of Appeals for the Federal Circuit in *In re Bilski.* Accordingly, Applicants respectfully request withdrawal of the rejection.

Claim 7 has been cancelled. Accordingly, the rejection thereof is moot.

35 USC 112, Second Paragraph

Claims 5 was rejected under 35 USC 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 5 has been amended to more clearly recite the subject matter of the invention. Applicants posit that Claim 5 now meets the requirements of 35 USC 112, second paragraph, and, accordingly, request withdrawal of the rejection.

35 USC 102

Claims 1-4 and 6-7 are rejected under 35 USC 102(b) as being anticipated by Cheng et al "Defensive Programming, in the Rapid Development of a Parallel Scientific Program, " hereinafter "Cheng".

Anticipation under 35 U.S.C. 102(b) requires that each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference, "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference", *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

Claim 1

Claim 1 as amended recites,

A method to secure an electronic assembly implementing a calculation process, the method comprising:

"performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature;

performing an elementary operation using a *super-function* operation acting from and/or to a larger set wherein a function f' is a *super-function* of a function f if

$h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F and a set F' wherein x is a member of E and f(x) is a member of the set F; and

performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature."

It may be useful to consider, what a *super-function*, as defined in the claim, accomplishes. By definition a *super-function f'* is a function that meets the requirement that $h_2(f'(h_1(x))) = f(x)$ wherein *h1* is a one-to-one mapping between the set of which *x* is a member and another set *E'* and *h2* is an onto mapping from the set F' to the set F. Using the *super-function* allows for a substitution of the calculation of the operation *f(x)* with the calculation that includes the *super-function*. If a normal encryption operation requires execution of the elementary operation f(x), that operation may be replaced with the operations h_1, *f'*, and h_2 in combination because of the identity relationship $h_2(f'(h_1(x))) = f(x)$.

Cheng does not teach or suggest an elementary operation using another "super function" operation and/or to a larger set as required by claim 1. Cheng is concerned with detecting errors due to bugs in the source code and is not concerned with detecting malicious attacks through the introduction of errors. Further, Cheng's aim is to optimize and reduce the time required to debug large programs. In order to accomplish this aim, Cheng uses checksums. "By comparing checksums produced in tracking the program and the checksums produced in tracing a reference copy of the program, errors can be rapidly localized when a program is modified, ported, put in parallel, or optimized for a particular machine" (pg. 665 Col 1 lines 9-12). In contrast, the aim of the Applicants invention is to detect an attack on an electronic assembly through the introduction of errors. This is a significant difference because simply using a checksum would not be sufficient to detect attacks.

35 USC 103

Claim 5 is rejected under 35 USC 103(a) as being unpatentable over Cheng in view of Roelse (US Patent Publication Number 2002/0101986 A1) hereinafter "Roelse". Applicants traverse the rejection.

Limitations similar to those found in Claim 5 as filed have been included, by this amendment, into Claim 1. As noted above, the *super-function* and the transformations that make the substitution $h_2(f'(h_1(x)))$ for f(x) possible are not taught or suggested by Cheng. Roelse also fails to teach or suggest these limitations.

The Examiner asserted that Roelse teaches "an elementary operation f of E in F is replaced by an operation f' of E' in F'" in the Abstract and Figure 3. Applicants disagree. To understand the meaning of *f'* it is necessary to consider the identity $h_2(f'(h_1(x))) = f(x)$ and the definitions of h_1 and h_2 that make that identity possible. As set forth in Claim 1, "$h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F, wherein x is a member of E and f(x) is a member of the set F." Thus, *f'* is a very particular function, namely, a *super-function* that satisfies the relationship $h_2(f'(h_1(x))) = f(x)$ given the definitions for h_1 and h_2.

Roelse teaches generation of a linear transformation that may be used, for example, in cryptography systems. Roelse describes the use of the linear transformation in a block-cipher encryption algorithm in which an input (X) is encrypted using a key (K) into an output E(X,K) (Roelse, Figure 1). Roelse describes the use of the invention in such a block-cipher system that is based on a round function *f* (Roesle, Paragraph [0017]. The exemplary block-cipher used by Roelse is a Feistel cipher consisting of sixteen rounds (like DES) (Roelse, Paragraph 0023). Figure 2 of Roelse illustrates the described Feistel cipher. As noted there, one aspect of the Feistel cipher is the function *f*, which in the example takes as inputs the

round key, K_i, and the right half of the output of the preceding round. Figure 3 is an illustration of the round function (Roesle, Paragraph 0012). As can be seen there, the function *f* consists of a key addition step 310, application of S-boxes 320, and a linear transformation 330 (it is the generation of this linear transformation that is the subject of the Roelse invention). There is nothing in these steps that may be considered a teaching of a *super-function* such that $h_2(f'(h_1(x))) = f(x)$. What in Figure 3 is supposed to stand for the function *f'*? What is the function *f(x)* that it is related to? Which are the transformations that make the relationship a *super-function* relationship? Applicants posit that considering these rhetorical questions will make it clear that there is no such relationship, that there is no *super-function* and that therefore, the Examiner's statement that "an elementary operation f of E in F is replaced by an operation f' of E' in F"' is incorrect.

Similarly, the Abstract of Roelse does not teach or suggest "an elementary operation f of E in F is replaced by an operation f' of E' in F'." The abstract, in rather incomprehensible terms, merely describes that the linear transformation (i.e., step 330 of Figure 3) is generated using an error-correcting code of some specification. The error-correcting code is in the form of a generator matrix having a particular form (identity matrix concatenated with a matrix of particular dimensions relating to the specification of the error-correcting code. The linear transformation is generated from the error-correcting code.

Nowhere in the Abstract is there reference to a function that has the property of a *super-function* as defined in Claim 1. Accordingly, for much the same reasons as argued with respect to Figure 3, the Examiner's statement that the Abstract of Roelse does not teach or suggest "an elementary operation f of E in F is replaced by an operation f' of E' in F"' is incorrect.

The Examiner goes on to state the notion that "E' and F' are super-sets of E and F, move from E to E' by one-to-one function h1" is taught at Roesle ¶3, Fig 5, element 516; ¶50; ¶52. Again, Applicants remind the Examiner that the claim as a whole must be considered and that the mapping *h1* must be considered in light of the identity $h_2(f'(h_1(x))) = f(x)$ which defines h1, f' and h2. That said, Roesle ¶3 is a background paragraph describing DES. There is nothing in there that suggests mapping from E to E'. In fact, the notion of relying on the identity $h_2(f'(h_1(x))) = f(x)$ to allow for the substitution of the left-side of the identity for the otherwise used f(x) is applicable to DES where f(x) is a round function in DES. However, DES by itself does not teach or suggest the replacement of f(x) with $h_2(f'(h_1(x)))$ and therefore, not the use of *h1* as defined by $h_2(f'(h_1(x))) = f(x)$. Figure 5, element 516 and ¶50 teach the addition of parity to a matrix. Applicants concede that that is a one-to-one mapping. However, as stated before, there is no indication that mapping is paired with a super-function and a second mapping (h2) to allow for the identity $h_2(f'(h_1(x))) = f(x)$. ¶52 teaches the addition of four columns to the matrix. "Preferably the four columns are randomly selected". While the addition of columns may be considered a one-to-one mapping, there is no indication that mapping is paired with a super-function and a second mapping (h2) to allow for the identity $h_2(f'(h_1(x))) = f(x)$. Accordingly, the Examiner's statement that "E' and F' are super-sets of E and F, move from E to E' by one-to-one function h1" is taught at Roesle ¶3, Fig 5, element 516; ¶50; ¶52 is incorrect.

Finally, the Examiner states "Move from F' to F by onto function h2 is taught in ¶3, Figure 4, ¶13, ¶58. As noted above, ¶3 merely describes DES and therefore can not be said to teach the mapping h2 as defined by the identity $h_2(f'(h_1(x))) = f(x)$; ¶13 merely introduces Figure 4 as showing an arrangement of an S-box construction. ¶58 describes how to construct the linear transformation matrix A using two permutation matrices P1

and P2 to achieve good diffusion properties. However, there is nothing in the paragraph that suggests a mapping h2 as defined by the identity $h_2(f'(h_1(x))) = f(x)$.

For the foregoing reasons, Claim 1 is patentable over the combination of Cheng and Roelse taken singly or in combination. Claim 5 depends from Claim 1, incorporates all the limitations of Claim 1, provides further unique and non-obvious combinations, and is patentable, at least, for the reasons given in support of Claim 1 and by virtue of such further combinations.

Claim 8 is rejected under 35 USC 103(a) as being unpatentable over Cheng in view of Borst et al "Cryptography on smart cards" hereinafter "Borst".

Claim 8 has been amended similarly as Claim 1. As argued in support of Claim 1, Cheng fails to teach or suggest "performing an additional calculation by a verification function on at least one intermediate result in order to obtain a calculation signature; performing an elementary operation using a *super-function* operation acting from and/or to a larger set wherein a function f' is *super-function* of a function f if $h_2(f'(h_1(x))) = f(x)$ wherein h_1 is a one-to-one mapping between a set E and a set E' and h_2 is an onto mapping of a set F' and a set F wherein x is a member of E and f(x) is a member of the set F; and performing the calculation by the verification function using the result obtained by the super function in order to obtain the calculation signature." Borst also fails to teach or suggest these limitations. Accordingly, the combination of Cheng and Borst fails to teach or suggest Claim 1. Claim 8, depending from Claim 1 and incorporating all the limitations thereof, is therefore, also patentable over the combination of Cheng and Borst.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: February 12, 2009

/Pehr Jansson/
Pehr Jansson

Registration No. 35,759

The Jansson Firm
9501 N. Capital of Texas Hwy #202
Austin, TX 78759
512-372-8440
512-597-0639 (Fax)
pehr@thejanssonfirm.com